COMPUTING LOCAL p-ADIC HEIGHT PAIRINGS ON HYPERELLIPTIC CURVES

JENNIFER S. BALAKRISHNAN AND AMNON BESSER

Abstract. We describe an algorithm to compute the local component at p of the Coleman-Gross p-adic height pairing on divisors on hyperelliptic curves. As the height pairing is given in terms of a Coleman integral, we also provide new techniques to evaluate Coleman integrals of meromorphic differentials and present our algorithms as implemented in Sage.

1. Introduction

For an elliptic curve over $\mathbb{Q}$, the classical Birch and Swinnerton-Dyer (BSD) conjecture predicts that a special value of its L-function can be given in terms of certain arithmetic invariants of the curve, one of which involves the canonical height pairing matrix of a basis of rational points. The p-adic analogue [MTT86] of the BSD conjecture makes a similar prediction, with the canonical height pairing replaced by a p-adic one [MT83]. These conjectures have natural generalizations to abelian varieties.

The p-adic height pairing was first defined by Schneider [Sch82] for abelian varieties and was extended to motives by Nekovář [Nek93]. For Jacobians of curves there is a third definition, due to Coleman and Gross [CG89], relying on Coleman's theory of p-adic integration [Col82, Col85, CdS88, Bes02]. This third definition of the height pairing is known to be equivalent to the previous ones [Bes04].

For the purpose of numerically verifying p-adic BSD type conjectures, it is important to have an effective algorithm for the computation of the p-adic height pairing. By the work of Kedlaya [Ked01] and Mazur, Stein, and Tate [MST06], we can easily compute p-adic heights on elliptic curves. Our work deals with the next logical step, p-adic height pairings on Jacobians of hyperelliptic curves.

The reason for treating Jacobians of hyperelliptic curves is that we have available the Coleman-Gross definition of the height pairing, which is much more concrete than previous definitions. The restriction to hyperelliptic curves is made primarily so that we may apply the recent algorithm [BBK10] for the computation of Coleman integrals on such curves, relying in turn on Kedlaya's work on the computation of the matrix of Frobenius on hyperelliptic curves [Ked01]. We note that generalizations of Kedlaya's work to other types of curves can be applied to generalize the results to these curves as well.

Coleman and Gross give a decomposition of the global p-adic height pairing as a sum of local height pairings at each prime. The local heights away from the prime p behave in much the same way as local archimedean heights, so the main interest lies in the primes above p, where Coleman integration is used. It is this last type of local height pairing which we aim to compute.

To fix ideas, consider a hyperelliptic curve C over $\mathbb{Q}_p$ with p a prime of good reduction. Then, for $D_1, D_2 \in \mathrm{Div}^0(C)$ with disjoint support, the Coleman-Gross p-adic height pairing at the prime p is given in terms of the Coleman integral

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1},$$

for an appropriately constructed differential ω_{D_1} associated to the divisor D_1. This last association is not straightforward and relies again on Coleman integration.

We say next to nothing in this work about the computation of local height pairings away from p. As mentioned before, this is not a p-adic problem and is shared with the computation of archimedean height pairings. In [Bes07] we suggested a method for treating this problem, which needed in particular some refined estimates of Kausz [Kau99]. In the meantime, we have learned that this problem is treated in the recent Ph.D. thesis of Müller [Mül10].

The structure of the paper is as follows: in Section 2, we review the work of Coleman and Gross [CG89] that constructs p-adic heights for curves, and in particular, defines the local contribution at p in terms of a Coleman integral. After a brief review of hyperelliptic curves in Section 3 we give, in Section 4, an overview of Coleman integration, where we discuss some known results for computing these integrals and describe a new construction that allows us to compute a broader class of integrals that the heights necessitate. We discuss the algorithm for computing the local height pairings in Section 5. In Section 6, we discuss our implementation of the algorithm in Sage along with error bounds on our results. We follow this in Section 7 with numerical examples illustrating our methods. We conclude in Section 8 by posing some questions arising from our work.

Acknowledgments. JB would like to thank Kiran Kedlaya for engaging in numerous helpful discussions and Liang Xiao for much constructive conversation. The implementation of this algorithm would not have been possible without David Roe and Robert Bradshaw, who laid much of the groundwork in Sage. Computations were done on `sage.math.washington.edu` (NSF Grant No. DMS-0821725), thanks to the generosity of William Stein. AB would like to thank the Institute for Advanced Study in Princeton where some preliminary work on this project, leading to the very rough sketch [Bes07], begun during the academic year 2006/2007, and the Isaac Newton Institute for Mathematical Sciences in Cambridge where some further work on this project was done in August 2009. JB's work was made possible by the NDSEG and NSF Graduate Fellowships. AB work was supported by the Bell companies Fellowship and the James D. Wolfensohn fund while at the Institute for Advanced Study and is presently supported by a grant from the Israel Science Foundation.

2. The p-adic height pairing

In this section we review the definition of the Coleman-Gross height pairing. As explained in the introduction, there are two required ingredients for making this definition: the theory of Coleman integration and a certain choice of a canonical form. These will be discussed in detail in a later section.

Suppose X/K is a curve defined over a number field K, with good reduction at primes above p. To define the height pairing

$$h : \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \to \mathbb{Q}_p\ ,$$

one needs the following data:

- A "global log"- a continuous idele class character
$$\ell : \mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p \ .$$
- For each $v|p$ a choice of a subspace $W_v \in H^1_{\mathrm{dR}}(X \otimes K_v / K_v)$ complementary to the space of holomorphic forms.

For the definition of the Coleman-Gross height we must insist that the local characters ℓ_v induced by ℓ, for $v|p$, are ramified in the sense that they do not vanish on the units in K_v.

From ℓ one deduces the following data:

- For any place $v \nmid p$ we have $\ell_v(\mathcal{O}_{K_v}^\times) = 0$ for continuity reasons, which implies that ℓ_v is completely determined by the number $\ell_v(\pi_v)$, where π_v is any uniformizer in K_v.
- For any place $v|p$ we can decompose
$$\begin{array}{ccc} \mathcal{O}_{K_v}^\times & \xrightarrow{\ell_v} & \mathbb{Q}_p \\ & {\scriptstyle \log_v} \searrow \quad \nearrow {\scriptstyle t_v} & \\ & K_v & \end{array}$$
where t_v is a $\mathbb{Q}_p$-linear map. Since we assume that ℓ_v is ramified it is then possible to extend
$$\log_v : K_v^\times \to K_v \tag{2.1}$$
in such a way that the diagram remains commutative.

Let us now describe the height pairing $h(D_1, D_2)$ for a pair of degree zero divisors D_1 and D_2 with disjoint support. The height pairing is a sum of local terms
$$h(D_1, D_2) = \sum_v h_v(D_1, D_2)$$
over all finite places v. The local terms depend only on the completion at v of K. Thus, let k be a local field of characteristic 0, with valuation ring $\mathcal{O}$, uniformizer π and let $F = \mathcal{O}/\pi\mathcal{O}$ be the residue field, with order q. Let C denote the curve X over the local field k. We shall assume that C has a k-rational point and that C has good reduction at π.

Let $\chi : k^* \to \mathbb{Q}_p$ be a continuous homomorphism, which is the local component of ℓ.

Proposition 2.1. *If* $\operatorname{char} F \neq p$, *and* $D_1, D_2 \in \operatorname{Div}^0(C)$ *have disjoint support, then there is a unique function* $\langle D_1, D_2 \rangle$ *that is continuous, symmetric, bi-additive,taking values in* $\mathbb{Q}_p$, *and satisfying*
$$\langle (f), D_2 \rangle = \chi(f(D_2)) \tag{2.2}$$
for $f \in k(C)^*$.

Proof. See [CG89, Prop 1.2]. In fact, one has [CG89, (1.3)]
$$h_v(D_1, D_2) = \ell_v(\pi_v) \cdot (D_1, D_2) \ . \tag{2.3}$$
Here, (D_1, D_2) denotes intersection multiplicity on a regular model of C over $\mathcal{O}$ of extensions of D_1 and D_2 to this model. To make this have the required properties

one of these extensions has to have zero intersection with all components of the special fibre. □

We now describe the local contribution at a place $v|p$.

Definition 2.2. A meromorphic differential on C over k is said to be of the *first kind* if it is holomorphic, of the *second kind* if it has residue 0 at every point, and of the *third kind* if it has a simple pole with residue in $\mathbb{Z}$, respectively.

Recall that the differentials of the second kind, modulo exact differentials, i.e., differentials of rational functions, form a finite dimensional k-vector space of dimension $2g$. It is canonically isomorphic to the first algebraic de Rham cohomology of C/k, $H^1_{\mathrm{dR}}(C/k)$, which is the hypercohomology group of the de Rham complex

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \Omega^1_{C/k} \longrightarrow 0$$

on C. We have a short exact sequence

$$0 \longrightarrow H^0(C, \Omega^1_{C/k}) \longrightarrow H^1_{\mathrm{dR}}(C/k) \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow 0, \tag{2.4}$$

where, relying on the description of de Rham cohomology in terms of forms of the second kind we have

- $H^0(C, \Omega^1_{C/k})$, the space of differentials of the first kind, is identified with its image. It has dimension g, and we will denote it $H^{1,0}_{\mathrm{dR}}(C/k)$.
- $H^1(C, \mathcal{O}_C)$ also has dimension g and may be canonically identified with the tangent space at the origin of the Jacobian of C, $J = \mathrm{Pic}^0(C)$.
- $H^1_{\mathrm{dR}}(C/k)$ has a canonical non-degenerate alternating form given by the algebraic cup product pairing

$$\begin{aligned} H^1_{\mathrm{dR}}(C/k) \times H^1_{\mathrm{dR}}(C/k) &\longrightarrow k \\ ([\mu_1], [\mu_2]) &\mapsto [\mu_1] \cup [\mu_2], \end{aligned}$$

  which can be described by the formula

$$[\mu_1] \cup [\mu_2] = \sum_P \mathrm{Res}_P(\mu_2 \int \mu_1), \tag{2.5}$$

  where μ_1, μ_2 are differentials of the second kind, with classes $[\mu_1]$ and $[\mu_2]$, respectively, in $H^1_{\mathrm{dR}}(C/k)$ and the sum is over all points in C. The residue does not depend on the choice of a particular local integral for μ_1 because μ_2 is of the second kind and has no residue at any point.

We will also need the theory of *Coleman integration*. Details will be discussed in Section 4 but for now it suffices to know that for each meromorphic form ω on C and to each $D \in \mathrm{Div}^0(C)$, the theory allows us to define the integral $\int_D \omega \in k$. In particular, for two k'-rational points P and Q, where k' is any finite extension of k, it allows us to define the integral $\int_P^Q \omega \in k'$. This construction is such that as Q (or P) varies, this last integral is expressed as a power series in Q which is locally convergent and whose differential is ω. For forms that have residues, the Coleman integral depends on the choice of a branch of the p-adic logarithm function. We fix this choice for the computation of the local height pairing to be the one determined in (2.1).

Let $T(k)$ denote the subgroup of differentials on C of the third kind. We have a *residue divisor homomorphism*

$$\mathrm{Res} : T(k) \to \mathrm{Div}^0(C), \qquad \mathrm{Res}(\omega) = \sum_P \mathrm{Res}_P\, \omega$$

where the sum ranges over all closed points of C. That the image is contained in $\mathrm{Div}^0(C)$ is just the residue theorem. By the residue divisor homomorphism, $T(k)$ fits into the following exact sequence:

$$0 \longrightarrow \Omega^1(C/k) \longrightarrow T(k) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(C) \longrightarrow 0. \tag{2.6}$$

We are interested in a particular subgroup of $T(k)$ whose elements are the logarithmic differentials, i.e., those of the form $\frac{df}{f}$ for $f \in k(C)^*$. We denote this subgroup as $T_l(k)$. Since $T_l(k) \cap H^{1,0}_{\mathrm{dR}}(C/k) = \{0\}$ and $\mathrm{Res}(\frac{df}{f}) = (f)$, we deduce from the sequence (2.6) the short exact sequence

$$0 \longrightarrow H^{1,0}_{\mathrm{dR}}(C/k) \longrightarrow T(k)/T_l(k) \longrightarrow J(k) \longrightarrow 0.$$

This sequence has a natural identification with the k-rational points of an exact sequence of commutative algebraic groups over k:

$$0 \longrightarrow H^0(C, \Omega^1_{C/k}) \longrightarrow E \longrightarrow J \longrightarrow 0,$$

where E is the universal extension of J by a vector group and $H^0(\Omega^1) \cong \mathbb{G}_a^g$. Since the Lie algebra of E is canonically isomorphic to $H^1_{dR}(C/k)$, the exact sequence (2.4) is the resulting exact sequence of Lie algebras over k.

Now as k is p-adic, we will make use of the fact that we have a logarithmic homomorphism defined on an open subgroup of the points of any commutative p-adic Lie group, G, to the points of its Lie algebra $\mathrm{Lie}(G)$. When $G = E$ or J, the open subgroup on which the logarithm converges has finite index, so the homomorphism can be uniquely extended to the entire group. We denote this extension as $\log_E$ or $\log_J$, respectively. Since the logarithm is functorial and equal to the identity on $H^0(C, \Omega^1_{C/k})$, we obtain the following:

Proposition 2.3. *There is a canonical homomorphism*

$$\Psi : T(k)/T_l(k) \longrightarrow H^1_{\mathrm{dR}}(C/k)$$

which is the identity on differentials of the first kind and makes the following diagram commute:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^{1,0}_{\mathrm{dR}}(C/k) & \longrightarrow & E(k) & \longrightarrow & J(k) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \Psi = \log_E} & & \downarrow{\scriptstyle \log_J} & & \\
0 & \longrightarrow & H^{1,0}_{\mathrm{dR}}(C/k) & \longrightarrow & H^1_{\mathrm{dR}}(C/k) & \longrightarrow & H^1(C, \mathcal{O}_{C/k}) & \longrightarrow & 0.
\end{array}$$

Note that the map Ψ takes a differential of the third kind on C to a differential of the second kind modulo exact differentials. It can be extended to a linear map from the k-vector space of all differentials on C/k to $H^1_{\mathrm{dR}}(C/k)$ by writing an arbitrary differential ν as a linear combination $\nu = \sum \alpha_i \mu_i + \gamma$, where μ_i is of the third kind, $\alpha_i \in \overline{k}$, and γ is of the second kind on C. We then define $\Psi(\nu) = \sum \alpha_i \Psi(\mu_i) + [\gamma]$.

The definition of the log map Ψ is not very useful for computations. An equivalent alternative definition has been given in [Bes00]. It is based on the notions of local and global symbols or indices.

Definition 2.4. For ω a meromorphic form and ρ a form of the second kind, we define the *global symbol* $\langle \omega, \rho \rangle$ as a sum of *local symbols* $\langle \omega, \rho \rangle_A$. We have

$$\langle \omega, \rho \rangle = \sum_A \langle \omega, \rho \rangle_A,$$

where

$$\langle \omega, \rho \rangle_A = \mathrm{Res}_A \left(\omega \left(\int \rho + \int_Z^A \rho \right) \right). \tag{2.7}$$

Note that the sum is taken over all points A where either ρ or ω has a singularity. Each local symbol $\langle \omega, \rho \rangle_A$ is computed in the local coordinates of A, and Z is a point that is fixed throughout the calculation of a single global symbol, which sets the constant of integration for the first indefinite integral of ρ. More precisely, we note that (2.7) is computed by rewriting ω and ρ using the local coordinates at A, computing the indefinite integral of ρ (as a formal power series, and in particular, not as a Coleman integral) and computing the Coleman integral of ρ from Z to A.

The following result [Bes00] reduces the computation of Ψ to the computation of global symbols.

Proposition 2.5. *Let ω be a meromorphic form and ρ a form of the second kind. Then $\langle \omega, \rho \rangle = \Psi(\omega) \cup [\rho]$.*

Proof. See [Bes00, Prop 4.10]. □

Now recall that we have at our disposal the complementary subspace $W = W_v$. It allows us to isolate a canonical form ω_D with residue divisor D as follows.

Definition 2.6. For any divisor D of degree 0 on C we let ω_D be the unique form of the third kind satisfying

$$\mathrm{res}(\omega_D) = D, \quad \Psi(\omega_D) \in W.$$

It is easy to see from the properties of Ψ that this indeed uniquely defines the form ω_D.

Definition 2.7. The local height pairing is defined by

$$h_v(D_1, D_2) := t_v \left(\int_{D_2} \omega_{D_1} \right)$$

(recalling that the supports of D_1 and D_2 are disjoint), where t_v is the trace map determined by the decomposition of ℓ_v.

Remark 2.8. In certain cases, there is a canonical complement W to $H^{1,0}_{\mathrm{dR}}(C/k)$ in $H^1_{\mathrm{dR}}(C/k)$. Namely, when C has good ordinary reduction, we may take W to be the unit root subspace for the action of Frobenius.

Some properties of the local height pairing are as follows:

Proposition 2.9. *The local height pairing $h_v(D_1, D_2)$ is continuous and bi-additive. It is symmetric if and only if the subspace W of $H^1_{\mathrm{dR}}(C/k)$ is isotropic with respect to the cup product pairing. Finally, the formula* (2.2) *holds.*

Proof. See [CG89, Prop 5.2]. □

3. Hyperelliptic curves

In this section we review relevant facts about algebraic and computational aspects of the theory of hyperelliptic curves.

Let us now suppose that C is a hyperelliptic curve. As k has characteristic not equal to 2, a hyperelliptic curve C over k of genus g is an algebraic curve given by the equation

$$y^2 = f(x)\ ,\ f(x) \in k[x], \tag{3.1}$$

where f has simple zeros. For our implementation in Sage, we shall further assume f to be monic and $\deg f = 2g + 1$.

The curve C is singular only at infinity (and non-singular when $g = 1$). To describe the neighborhood of infinity we normalize the curve there and obtain the *equation at infinity*

$$t^2 = sf^{\mathrm{rev}}(s) \text{ with } x = \frac{1}{s},\ \ y = \frac{t}{s^{g+1}}, \tag{3.2}$$

where $f^{\mathrm{rev}}(s) = s^{2g+1}f(1/s)$ is the reversed polynomial. The point at infinity corresponds in these coordinates to both s and t being 0. Furthermore, t has a simple zero and s has a double zero at this point.

As is well-known, the first de Rham cohomology of C has a basis consisting of the forms of the second kind

$$\omega_i := \frac{x^i dx}{2y} \text{ for } i = 0, \ldots, 2g-1.$$

We will denote this basis as

$$\mathcal{B} = \left\{ \frac{dx}{2y}, \frac{xdx}{2y}, \ldots, \frac{x^{2g-1}dx}{2y} \right\}. \tag{3.3}$$

If we make the change of coordinates (3.2) we see that these are transformed as follows:

$$\frac{x^i dx}{2y} \mapsto -s^{g-1-i}\frac{ds}{2t}.$$

Since s has a double zero at the point at infinity one sees that these forms are holomorphic for $i = 0, \ldots, g-1$ and meromorphic otherwise.

We finally recall the *hyperelliptic involution* w defined by $w(x, y) = (x, -y)$.

4. Coleman integrals

Here we review the relevant background on Coleman integrals and describe new techniques to handle Coleman integrals of meromorphic differentials with poles in non-Weierstrass residue discs. This gives us the necessary tools to present our algorithm to compute local heights.

4.1. **Differentials of the second kind.** The foundational reference for this is [Col85]. A more expanded version of our presentation can be found in [BBK10].

Let ω be a 1-form, with $(\omega)_\infty$ denoting its polar support. For $P, Q \in C(k)$, Coleman integration allows us to compute $\int_P^Q \omega \in k$.

Theorem 4.1. *Let μ, ν be 1-forms on C and $P, Q, R \in C(k)$. The (definite) Coleman integral has the following properties:*

(1) *Linearity: $\int_P^Q (a\mu + b\nu) = a\int_P^Q \mu + b\int_P^Q \nu$, for $P, Q \notin (\mu)_\infty \cup (\nu)_\infty$.*

(2) *Additivity:* $\int_P^R \mu = \int_P^Q \mu + \int_Q^R \mu$, *for* $P, Q, R \notin (\mu)_\infty$.
(3) *Change of variables: If* C' *is another curve and* $\phi : C \to C'$ *a rigid analytic map between wide opens then* $\int_P^Q \phi^* \mu = \int_{\phi(P)}^{\phi(Q)} \mu$ *if* $\phi(P), \phi(Q) \notin (\mu)_\infty$.
(4) *Fundamental theorem of calculus:* $\int_P^Q df = f(Q) - f(P)$ *for* f *a meromorphic function* f *on a wide open subset.*

Proof. See [Col85, Thm 2.3, Prop 2.4, Thm 2.7] for details. □

Thus writing

$$\omega = df + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1},$$

where f is a function and $c_i \in k$, we see that the problem of computing $\int_P^Q \omega$ reduces to computing the Coleman integral of a basis differential, $\int_P^Q \omega_i$.

For hyperelliptic curves, Coleman integration can be performed numerically. For simplicity we describe things only over $\mathbb{Q}_p$ although things work in complete generality (see [BBK10] and also [Bes10] where a slightly different but related version, which was implemented in [Gut06], is described).

Let us recall the following algorithms (Algorithms 8 and 11, respectively) from [BBK10]. Throughout, let ϕ denote a p-power lift of Frobenius.

Algorithm 4.2 (Tiny Coleman integrals)**.**
Input:

- Points $P, Q \in C(\mathbb{Q}_p)$ in the same residue disc (neither equal to the point at infinity).
- A basis differential ω_i.

Output: The integral $\int_P^Q \omega_i$.
The algorithm:

(1) Construct a linear interpolation from P to Q. For instance, in a non-Weierstrass residue disc, we may take

$$x(t) = (1-t)x(P) + tx(Q)$$
$$y(t) = \sqrt{f(x(t))},$$

where $y(t)$ is expanded as a formal power series in t.
(2) Formally integrate the power series in t:

$$\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^1 \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt.$$

Algorithm 4.3 (Coleman integration in non-Weierstrass discs)**.**
Input:

- The basis differentials $\{\omega_i\}_{i=0}^{2g-1}$.
- Points $P, Q \in C(\mathbb{Q}_p)$ in non-Weierstrass residue discs.

Output: The integrals $\{\int_P^Q \omega_i\}_{i=0}^{2g-1}$.
The algorithm:

(1) Calculate the action of Frobenius on each basis element :

$$\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

(2) By change of variables (see Remark 4.4), we obtain

$$\sum_{j=0}^{2g-1}(M-I)_{ij}\int_P^Q \omega_j = f_i(P) - f_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i. \tag{4.1}$$

As the eigenvalues of the matrix M are algebraic integers of $\mathbb{C}_p$-norm $p^{1/2} \neq 1$ (see [Ked01, §2]), the matrix $M - I$ is invertible, and we may solve (4.1) to obtain the integrals $\int_P^Q \omega_i$.

Remark 4.4. We obtain (4.1) as follows. By change of variables,

$$\begin{aligned}\int_{\phi(P)}^{\phi(Q)} \omega_i &= \int_P^Q \phi^*(\omega_i) \\ &= \int_P^Q (df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j) \\ &= f_i(Q) - f_i(P) + \sum_{j=0}^{2g-1} M_{ij}\int_P^Q \omega_j.\end{aligned}$$

Adding $\int_P^{\phi(P)} \omega_i + \int_{\phi(Q)}^Q \omega_i$ to both sides of this equation yields

$$\int_P^Q \omega_i = \int_P^{\phi(P)} \omega_i + \int_{\phi(Q)}^Q \omega_i + f_i(Q) - f_i(P) + \sum_{j=0}^{2g-1} M_{ij}\int_P^Q \omega_j,$$

which is equivalent to (4.1).

4.2. **Meromorphic differentials.** The above approach does not work for a meromorphic differential with poles in non-Weierstrass residue discs. We provide a new approach for dealing with this case (again we describe things only over $\mathbb{Q}_p$ but things work in general). Let ω be such a differential. As before, if R, S are points in the same non-Weierstrass residue disc (different from those discs containing the poles of ω), then $\int_S^R \omega$ is just a tiny integral, which can be computed as in Algorithm 4.2. Let us now suppose that R, S are in different non-Weierstrass residue discs.

Algorithm 4.5 (Coleman integration: differential with poles in non-Weierstrass discs)**.**
Input:

- The differential ω with residue divisor $(P) - (Q)$, with non-Weierstrass points $P, Q \in C(\mathbb{Q}_p)$.
- Points $R, S \in C(\mathbb{Q}_p)$ in distinct non-Weierstrass residue discs.

Output: The integral $\int_S^R \omega$.
The algorithm:

(1) Let $\alpha = \phi^*(\omega) - p\omega$. Using the methods of Section 5.2, compute $\Psi(\omega)$. Using this, compute $\Psi(\alpha)$ as $\phi^*(\Psi(\omega)) - p\Psi(\omega)$.
(2) Let β be a form with residue divisor $(R) - (S)$. Compute $\Psi(\beta)$.
(3) Compute the cup product $\Psi(\alpha) \cup \Psi(\beta)$ (see Section 5.1 for more details).
(4) Evaluate the tiny integrals $\int_{\phi(S)}^S \omega$ and $\int_R^{\phi(R)} \omega$.

(5) Let $\mathcal{S}$ be the set of Weierstrass points and poles of α. For each point $A \in \mathcal{S}$, expand $\alpha \int \beta$ in terms of the local coordinate at A and find the residue at A. Compute the sum

$$\sum_{A \in \mathcal{S}} \mathrm{Res}_A(\alpha \int \beta).$$

(6) By Coleman reciprocity (see Remark 4.6), recover the desired integral:

$$\int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum_{A \in \mathcal{S}} \mathrm{Res}_A\left(\alpha \int \beta\right) - \int_{\phi(S)}^{S} \omega - \int_R^{\phi(R)} \omega\right). \tag{4.2}$$

Remark 4.6. We obtain (4.2) as follows:

$$\begin{aligned} \int_S^R \alpha &= \int_S^R \phi^*\omega - p\int_S^R \omega \\ &= \int_{\phi(S)}^{\phi(R)} \omega - p\int_S^R \omega \\ &= (1-p)\int_S^R \omega + \left(\int_{\phi(S)}^{S} \omega + \int_R^{\phi(R)} \omega\right). \end{aligned} \tag{4.3}$$

As β is a form with residue divisor $(R) - (S)$, by Coleman reciprocity [Col89, Theorem 5.2], we compute the LHS of (4.3) to be

$$\sum_{A \in \mathcal{T}} \mathrm{Res}_A\left(\beta \int \alpha\right) = \Psi(\alpha) \cup \Psi(\beta) - \sum_{A \in \mathcal{S}} \mathrm{Res}_A\left(\alpha \int \beta\right),$$

where $\mathcal{T}$ is the set of Weierstrass points and poles of β. We then have

$$\int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum_{A \in \mathcal{S}} \mathrm{Res}_A\left(\alpha \int \beta\right) - \int_{\phi(S)}^{S} \omega - \int_R^{\phi(R)} \omega\right).$$

Remark 4.7. In practice, the computation in Step 5 of Algorithm 4.5 is the slowest part of the algorithm, as it involves high-precision local calculations over all poles of α and all Weierstrass points of the curve. However, since $\sum_{T \in U} \mathrm{Res}_T(\alpha) = 0$ in each residue disc U, for the Weierstrass discs, we do not need a constant of integration. For the poles of α, we may choose one constant of integration within each residue disc. More precisely, if P and Q are in separate residue discs, we compute

$$\begin{aligned} \sum_{A \in U_P} \mathrm{Res}_A\left(\alpha \int \beta\right) &= \mathrm{tr}_{k(x(P_1))/k}\left(\mathrm{Res}_{P_1}\left(\alpha \int_P^{P_1} \beta\right)\right) = \mathrm{tr}_{k(x(P_1))/k}\left(\int_P^{P_1} \beta\right), \\ \sum_{A \in U_Q} \mathrm{Res}_A\left(\alpha \int \beta\right) &= \mathrm{tr}_{k(x(Q_1))/k}\left(\mathrm{Res}_{Q_1}\left(\alpha \int_Q^{Q_1} \beta\right)\right) = \mathrm{tr}_{k(x(Q_1))/k}\left(-\int_Q^{Q_1} \beta\right), \end{aligned}$$

where P_1 (resp, Q_1) is a root of α in the residue disc of P (resp Q).

5. The local height pairing at primes above p

In this section we will explain the algorithm that computes the local height pairing at a prime above p for degree zero divisors on the hyperelliptic curve C. Recall that we have as additional data the complementary subspace W and the character χ from which we deduce a branch of the logarithm to be used in Coleman integration and the trace map t_v (we keep the subscript v at some places for clarity, even though it now serves no purpose).

Let D_1 and D_2 be two divisors of degree 0 on C. Our main algorithm computes the local height pairing $h_v(D_1, D_2)$. It may be described in two steps

- Compute the height pairing in the case where D_1 and D_2 are anti-symmetric with respect to the hyperelliptic involution (Algorithm 5.8)
- Compute the height pairing in the general case using the first case (Algorithm 5.7).

Before discussing either algorithm, we begin with some general notes about the representation of divisors on hyperelliptic curves (see [Kob98, App §5-6]).

Recall that a divisor of degree 0 on C may be written in the form

$$D = \sum m_i P_i - \left(\sum m_i\right)(\infty).$$

Definition 5.1. A divisor D as above is called *semi-reduced* if the following conditions are satisfied:

- $m_i \geq 0$
- If P_i is in the support of D, then $-P_i$ is not, unless $P_i = -P_i$ in which case $m_i = 1$.

A semi-reduced divisor is called *reduced* if in addition

- $\sum m_i \leq g$.

One may represent a semi-reduced divisor D by a pair of polynomials $a(x), b(x)$ with $\deg(b) < \deg(a)$ such that

- The projection of $\sum m_i P_i$ on $\mathbb{P}^1$ is the zero divisor of $a(x)$.
- $b(x)$ is an interpolation polynomial with the property that for $P_i = (x_i, y_i)$ we have $b(x_i) = y_i$.

The condition that D is reduced is equivalent to having $\deg(a) \leq g$.

Remark 5.2. One can associate b uniquely to the divisor by insisting that $a(x)|(b(x)^2 - f(x))$. This would be less important for us and there are cases we may not achieve this.

Definition 5.3. Let us denote by (a, b) the semi-reduced divisor determined by the pair of polynomials a and b and call (a, b) the standard representation of the divisor.

It is known that any degree zero divisor D on C is equivalent to a unique reduced divisor. Furthermore, the reduction is effective. More precisely, passing from an arbitrary divisor to a semi-reduced one is just a question of adding or subtracting divisors of functions pulled back from $\mathbb{P}^1$ while passing from a semi-reduced divisor to a reduced divisor has an effective algorithm described in [Kob98, App, Alg 2 and Thm 7.2]. Since we know our height pairing satisfies (2.2) by Proposition 2.9, which easily allows to pass from a divisor to an equivalent divisor in the pairing there is no harm in assuming that our divisors are reduced.

Unfortunately for us, reduced divisors are not sufficient. The reason is that since they always have a component at infinity, two such divisors cannot have disjoint support unless one of them is trivial. For this reason we will work with the difference of two reduced divisors.

Definition 5.4. The divisor denoted $(a,b)-(c,d)$, where a and c are polynomials of the same degree $\leq g$, stands for the difference of the reduced divisors defined by (a,b) and (c,d).

We always assume that the two divisors defined by (a,b) and (c,d) have no common components. If there are common components they can be cancelled out.

We will mostly work with antisymmetric divisors. Given any zero divisor D, the divisor $D-w^*D$ is antisymmetric. Conversely, any antisymmetric divisor is obtained in this way. It follows easily that any antisymmetric divisor is equivalent to $D-w^*D$ for a reduced divisor. There may be several representations in this form for a given divisor, however, there is just one containing no points P_i with $P_i=-P_i$. In the representation (a,b) for D this is equivalent to having a prime to f.

Definition 5.5. The standard representation of an anti-symmetric divisor is

$$[a,b]:=D-w^*D$$

with D a reduced divisor given in the form (a,b). It is a reduced standard representation if a is prime to f.

Note that with anti-symmetric divisors the standard representation suffices because they do not have components at infinity. Thus, $[a_1,b_1]$ and $[a_2,b_2]$ have disjoint support if and only if a_1 and a_2 are relatively prime.

We now describe Algorithm 5.7. For any divisor D we have a decomposition, with rational coefficients

$$D=\frac{1}{2}D^+ + \frac{1}{2}D^-, \qquad D^+=D+w^*(D)\ ,\ D^-=D-w^*(D). \tag{5.1}$$

Lemma 5.6. *Suppose D is given by the representation $(a,b)-(c,d)$. Then, the divisor D^- is just $[a\cdot c,e]$ in terms of Definition 5.5, where e is obtained by solving a Chinese Remainder Theorem problem to be congruent to b modulo a and to $-d$ modulo c.*

Proof. If a is prime to c this is clear. In general, suppose $(x-\alpha)$ has multiplicity m in a and n in c. We may assume $m\geq n$. Since we are assuming (a,b) and (c,d) have no common components, it follows that $D-w^*(D)$ is going to have the two summands $(m+n)[(\alpha,b(\alpha))-(\alpha,-b(\alpha)]$, and $m+n$ is indeed the multiplicity of ac in α (it seems though that we can only solve the Chinese remainder problem modulo the least common multiple of a and c). □

On the other hand, D^+ is nothing but the divisor of the rational function $\frac{a(x)}{c(x)}$ considered as a rational function on C. It follows from the fact that (2.2) is satisfied by Proposition 2.9 that for any $E\in \mathrm{Div}^0(C)$ we have

$$h_v(D^+,E)=h_v(E,D^+)=\chi\left(\frac{a}{c}(E)\right), \tag{5.2}$$

where $\frac{a}{c}(E)$ means as usual the product of the values of $\frac{a}{c}$ on the x-coordinates of the points making up E with the appropriate multiplicities. An easy consequence

of this formula is that

$$h_v(D^+, E) = h_v(E, D^+) = 0 \quad \text{if } E \text{ is antisymmetric.} \tag{5.3}$$

Consider now two divisors D_1 and D_2 in $\mathrm{Div}^0(C)$. Decomposing into plus and minus parts it follows from (5.3) that

$$h_v(D_1, D_2) = \frac{1}{4} h_v(D_1^+, D_2^+) + \frac{1}{4} h_v(D_1^-, D_2^-). \tag{5.4}$$

The first term can be computed using (5.2), while the second term is a height pairing between anti-symmetric divisors. This immediately gives the following algorithm.

Algorithm 5.7 (p-adic height pairing for general divisors)**.**
Input:

- The subspace W, branch of logarithm and trace map t.
- Divisors D_1 and D_2 with disjoint support given as

$$D_1 = (a_1, b_1) - (c_1, d_1)$$
$$D_2 = (a_2, b_2) - (c_2, d_2).$$

Output: The local height pairing $h_v(D_1, D_2)$.
The algorithm:

(1) Compute expressions for the divisors D_1^- and D_2^- using Lemma 5.6.
(2) Compute using (5.2),
$$h_v(D_1^+, D_2^+) = \chi((a_1/c_1)(D_2^+)).$$
(3) Compute, using Algorithm 5.8, the local height pairing for anti-symmetric divisors $h_v(D_1^-, D_2^-)$.
(4) Substitute in (5.4) to obtain $h_v(D_1, D_2)$.

We next turn to Algorithm 5.8 for the case of anti-symmetric divisors D_1 and D_2. First of all, we have to introduce yet another decomposition. The algorithm behaves differently with respect to parts that reduce to the Weierstrass points (Weierstrass divisors) and those which do not. We can decompose a divisor D into the sum of its Weierstrass part $D^{\mathbf{w}}$ and its non-Weierstrass part $D^{\mathbf{nw}}$. Then, in a similar way to (5.4) we have the decomposition

$$h_v(D_1, D_2) = h_v(D_1, D_2^{\mathbf{w}}) + h_v(D_1^{\mathbf{w}}, D_2^{\mathbf{nw}}) + h_v(D_1^{\mathbf{nw}}, D_2^{\mathbf{nw}}). \tag{5.5}$$

We now give the algorithm and later we discuss each step with some more details.

Algorithm 5.8 (p-adic height pairing for anti-symmetric divisors)**.**
Input:

- The subspace W, branch of logarithm and trace map t.
- Anti-symmetric divisors D_1 and D_2 given in standard representation (a_1, b_1), (a_2, b_2).

Output: The local height pairing $h_v(D_1, D_2)$.
The algorithm:

(1) Compute the cup product matrix for a basis of $H^1_{\mathrm{dR}}(C/k)$, as in Section 5.1.
(2) Compute $D_1^{\mathbf{w}}$ and $D_1^{\mathbf{nw}}$.
(3) Write down forms $\nu_1^{\mathbf{w}}$ and $\nu_1^{\mathbf{nw}}$ with residue divisors $D_1^{\mathbf{w}}$ and $D_1^{\mathbf{nw}}$, respectively.

(4) Compute the form $\omega_{D_1^{\mathbf{w}}}$ and a holomorphic form η such that
$$\omega_{D_1^{\mathbf{nw}}} = \nu_1^{\mathbf{nw}} - \eta.$$
(5) Compute the tiny Coleman integral $h_v(D_1, D_2^{\mathbf{w}}) = t(\int_{D_2^{\mathbf{w}}}(\omega_{D_1^{\mathbf{w}}} + \nu_1^{\mathbf{nw}} - \eta))$.
(6) Compute the Coleman integral $h_v(D_1^{\mathbf{w}}, D_2^{\mathbf{nw}}) = t(\int_{D_2^{\mathbf{nw}}} \omega_{D_1^{\mathbf{w}}})$.
(7) Compute the Coleman integral $h_v(D_1^{\mathbf{nw}}, D_2^{\mathbf{nw}}) = t(\int_{D_2^{\mathbf{nw}}} \nu_1^{\mathbf{nw}} - \int_{D_2^{\mathbf{nw}}} \eta)$.
(8) Compute $h_v(D_1, D_2)$ using (5.5).

We now add some further details on each step in this algorithm.

5.1. **Computing cup products.** We first compute the cup product between any two elements of the standard basis (3.3) for $H^1_{\mathrm{dR}}(X/k)$. This is easily done using the formula (2.5).

We can be a bit more precise as follows.

Definition 5.9. The *cup product matrix* associated to C with respect to $\mathcal{B}$ is the $2g \times 2g$ matrix with entry $a_{i,j}$ given by the cup product of differentials $[\omega_{i-1}] \cup [\omega_{j-1}]$, normalized so that $[\omega_{i-1}] \cup [\omega_{j-1}] = \mathrm{Res}(\omega_{j-1} \int \omega_{i-1})$.

By computing in the local coordinates at infinity, we may record the following

Lemma 5.10. *The cup product matrix for C with respect to $\mathcal{B}$ satisfies the following properties:*

(1) *Anti-diagonal elements are given by the sequence*
$$\left\{ \frac{1}{2g-1}, \frac{1}{2g-3}, \ldots, \frac{1}{3}, 1, -1, -\frac{1}{3}, \ldots, -\frac{1}{2g-1} \right\}.$$
(2) *Entries above the anti-diagonal are 0.*
(3) *Diagonal elements are 0.*

Example 5.11. The cup product matrix with respect to $\mathcal{B}$ for an elliptic curve is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Note that the subspace spanned by $\frac{xdx}{2y}$ is isotropic. In particular, for genus 1, we may take $H^{1,0}_{\mathrm{dR}}(C/k)$ spanned by ω_0 and W spanned by ω_1, and we need not require p to be a prime of ordinary reduction for the pairing to be symmetric.

5.2. **The map Ψ.** We compute Ψ of a differential ω by writing
$$\Psi(\omega) = c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1},$$
and solving for the coefficients c_i. This is done by considering a linear system involving global symbols and cup products:
$$\langle \omega, \omega_j \rangle = \Psi(\omega) \cup [\omega_j] = \sum_{i=0}^{2g-1} c_i([\omega_i] \cup [\omega_j]).$$

Recall that as in Definition 2.4, we calculate the global symbol as a sum of local symbols, each of which involves a Coleman integral and a calculation in local coordinates. This computation is actually much simpler:

Proposition 5.12. *Suppose ω is a form of the third kind with residue divisor D which does not contain ∞. Then we have*
$$\langle \omega, \omega_i \rangle = \int_D \omega_i + \mathrm{Res}_\infty \left(\omega \int \omega_i \right),$$
where the residue at ∞ is computed by taking any antiderivative of ω_i.

Proof. The sum of local symbols is over all points where either ω or ω_i has a singularity. These are the points in the support of D and possibly the point ∞. Since ω has a simple pole at each point P in the support of D, the local symbol is simply the multiplicity of D at P times $\int_Z^P \omega_i$ (where Z is a fixed point throughout the global symbol calculation). Summing over all points gives $\int_D \omega_i$. On the other hand, since we are assuming that ω is holomorphic at ∞, the choice of the constant of integration for ω_i at ∞ does not matter. □

Now letting N denote the cup product matrix, we have

$$\Psi(\omega) = N^{-1} \begin{pmatrix} \langle \omega, \omega_0 \rangle \\ \vdots \\ \langle \omega, \omega_{2g-1} \rangle \end{pmatrix}.$$

5.3. **Decomposing a divisor D into $D^{\mathbf{w}}$ and $D^{\mathbf{nw}}$.** This is very easy to do. When the divisor is given in standard form $[a, b]$ one just reduces a modulo the prime π, picks up the part that reduces to Weierstrass points by taking the greatest common divisor with the reduction of f, and then applies a Hensel lift to get the factor $a^{\mathbf{w}}$ of a corresponding to the points reducing to Weierstrass. Then we have $a^{\mathbf{nw}} = a/a^{\mathbf{w}}$ and the divisor decomposition is deduced from that.

5.4. **A form with the required residue divisor.** This is an easy task with the following:

Proposition 5.13. *Let the anti-symmetric divisor D be given in standard representation $[a, b]$. The differential form*

$$\omega = \frac{a'(x)b(x)dx}{a(x)y}$$

has simple poles and its residue divisor is D.

Proof. Suppose that $(a, b) = \sum m_i P_i - (\sum m_i)(\infty)$. We can write $\omega = (b/y)\,\mathrm{dlog}(a)$. The form $\mathrm{dlog}(a)$ has simple poles at $\pm P_i$ with residue m_i while b/y has value 1 at P_i and value -1 at $-P_i$. On the other hand we can also write $\omega = (a'b/a)(\frac{dx}{2y})$ and since $\frac{dx}{2y}$ is holomorphic, it follows that ω has no poles where a does not vanish. Finally, it is easy to see that ω does not have a pole at infinity. □

5.5. **Finding ω_D for a Weierstrass divisor D.** Suppose we have already written down a form whose residue divisor is D. Since the singularities of the form are contained in the Weierstrass residue discs, it is amenable to the reduction algorithm done in Kedlaya's algorithm [Ked01]. This means that we may compute a representation of ω as a linear combination of the basis $\mathcal{B}$ plus an exact differential dg. Since it follows that $\Psi(\omega)$ is just the above combination of basis elements, we need only subtract the appropriate combination of holomorphic basis elements to make it reside in W.

5.6. **Finding ω_D for a non-Weierstrass divisor D.** We start with a form ω whose residue divisor is D. We compute $\Psi(\omega)$ as in Section 5.2. All that is left to do is to let η be the projection of $\Psi(\omega)$ on $H^{1,0}_{\mathrm{dR}}$ along W.

5.7. **Integration when D_2 reduces to Weierstrass points.** Suppose that the points of D_2 reduce to the Weierstrass points. Since D_2 is anti-symmetric, this means that in computing the integral we need to take the sum of differences over pairs of points $\pm P$ which reduce to the same point. This is a sum of tiny integrals.

5.8. **Computation when D_1 is Weierstrass and D_2 is not.** In this case, we are given, by the previous reduction, the form ω_{D_1} as a combination $\sum \alpha_i \omega_i + dg$. Thus $\int_{D_2} \omega_{D_1} = \sum \alpha_i \int_{D_2} \omega_i + g(D_2)$. Since the points of D_2 are in the domain where the integrals of the ω_i may be computed, this is a standard computation.

5.9. **Computation when both divisors are non-Weierstrass.** In this case, ω_{D_1} is given in the form $\nu_1 - \eta$, where ν_1 is a form with residue divisor D_1 and η is holomorphic. The integral of η poses no problems while that of ν_1 is discussed in Subsection 4.2.

6. Implementation notes

In this section, we discuss the choices made in our Sage [S+10] implementation and give error estimates on the precision of our results. We work over $\mathbb{Q}_p$ with a precision of n digits; note that if one desires an answer with n digits of precision, one has to start with a larger working precision, as seen below.

We only discuss the computation for anti-symmetric divisors, as the extension to general divisors is trivial, as discussed in Section 5. Furthermore, our implementation assumes that the divisors are of the form $(P) - (-P)$ for a $\mathbb{Q}_p$-rational point P, as it is then quite easy to consider cases when the divisor is a sum of such expressions. Finally, all computations are done with respect to a particular choice of the complementary subspace W, which we describe below.

6.1. **Auxiliary choices.** Our algorithm relies on the splitting

$$H^1_{\mathrm{dR}}(C/k) \simeq H^{1,0}_{dR}(C/k) \oplus W,$$

which allows us to write

$$\log(\nu_1) = \eta + \log(\omega_{D_1}),$$

where η is holomorphic, and $\log(\omega_{D_1}) \in W$.

As noted in Example 5.11, when $g = 1$, we may simply take $H^{1,0}_{\mathrm{dR}}(C/k)$ spanned by ω_0 and W spanned by ω_1. Note that for genus $g > 1$ it does not suffice to take W spanned by $\omega_g, \omega_{g+1}, \ldots, \omega_{2g-1}$, as the resulting subspace is not necessarily isotropic. While the local height is independent of basis, it is not independent of the choice of W. For the local height to be symmetric, it is necessary that W be an isotropic subspace. For $g > 1$, we thus further require that p be a prime of *ordinary* reduction, so that W can be chosen to be the unit root subspace. Generalizing [MST06], we compute a basis for W as follows:

Proposition 6.1. *Let n be the working precision in the underlying base ring $\mathbb{Z}_p$, so that all computations are done modulo p^n. Let* Frob *denote the matrix of a p-power lift of Frobenius, as acting on the standard basis $\mathcal{B}$ of $H^1_{\mathrm{dR}}(C/k)$. Then $\{\mathrm{Frob}^n \omega_g, \mathrm{Frob}^n \omega_{g+1}, \ldots, \mathrm{Frob}^n \omega_{2g-1}\}$ is a basis for W.*

Proof. With the integral structure provided by crystalline cohomology, it is well known that Frob maps the holomorphic forms to p times the integral structure. Thus, with W the unit root part decomposing a vector v into $\omega + \eta$ with $\omega \in W$ and η holomorphic it is easy to see that $\mathrm{Frob}^n v$ is in $W + p^n$ times the integral

structure. In other words, up to the prescribed precision, $\mathrm{Frob}^n v$ lies in W. On the other hand, Frob is invertible so starting with g independent vectors modulo the holomorphic differentials one gets g independent vectors in W. □

6.2. **Precision.** Broadly speaking, the p-adic precision of a local height depends on two types of calculation:

(1) Coleman integrals of basis differentials (or otherwise "nice" differentials – e.g., holomorphic in the discs corresponding to the limits of integration) and
(2) expansion of local coordinates at a point.

Each key step of the algorithm in Section 4.5 can be categorized as depending on one or both of these:

- $\Psi(\omega)$ needs the cup product matrix (local coordinates) and local symbols (Coleman integrals of basis differentials)
- $\int \eta$ is a sum of Coleman integrals of basis differentials
- $\int \omega$ is defined in terms of
  - tiny integrals (Coleman integrals of a "nice" differential),
  - sums of residues of Laurent series (local coordinates), and
  - $\Psi(\alpha)$, $\Psi(\beta)$ (as above).

6.2.1. *Precision of Coleman integrals.* For more details on the rigorous computation of Coleman integrals, see [BBK10]. We recall the following results ([BBK10, Props 18-19]):

Proposition 6.2. *Let $\int_P^Q \omega$ be a tiny integral in a non-Weierstrass residue disc, with P, Q defined over an unramified extension of $\mathbb{Q}_p$ and accurate to n digits of precision. Let $(x(t), y(t))$ be the local interpolation between P and Q defined by*

$$x(t) = x(P)(1-t) + x(Q)t = x(P) + t(x(Q) - x(P))$$
$$y(t) = \sqrt{f(x(t))}.$$

Let $\omega = g(x,y)dx$ be a differential of the second kind such that $h(t) = g(x(t), y(t))$ belongs to $\mathcal{O}[[t]]$. If we truncate $h(t)$ modulo t^m, then the computed value of the integral $\int_P^Q \omega$ will be correct to $\min\{n, m+1-\lfloor \log_p(m+1) \rfloor\}$ digits of (absolute) precision.

Proposition 6.3. *Let $\int_P^Q \omega$ be a Coleman integral, with ω a differential of the second kind and with P, Q in non-Weierstrass residue discs, defined over an unramified extension of $\mathbb{Q}_p$, and accurate to n digits of precision. Let* Frob *be the matrix of the action of Frobenius on the basis differentials. Set $B = \mathrm{Frob}^t - I$, and let $m = v_p(\det(B))$. Suppose the relevant tiny integrals have series expansions truncated modulo t^{n-1}. Then the computed value of the integral $\int_P^Q \omega$ will be accurate to $n - \max\{m, \lfloor \log_p n \rfloor\}$ digits of precision.*

We will now carefully review the precision of each of the objects we computed, as an expansion of the overview in Section 6.2. Let ω be a differential with residue divisor

$$D_1 = (P) - (-P)$$

and β a differential with residue divisor

$$D_2 = (Q) - (-Q).$$

The precision of $\Psi(\omega)$ (and $\Psi(\beta)$) just depends on the Coleman integral involved, as the residue can just be read off of the differential.

After computing $\Psi(\omega)$ with respect to the standard basis of $H^1_{\mathrm{dR}}(C)$, we fix a splitting of $H^1_{\mathrm{dR}}(C/k)$ into $H^{1,0}_{\mathrm{dR}}(C/k) \oplus W$, which gives η and $\omega_{D_1} = \omega - \eta$. Since the height pairing is given by $\int \omega_{D_1}$, we need to compute the integrals $\int \omega$ and $\int \eta$.

The integral $\int \eta$ is just a linear combination of the integrals of holomorphic basis differentials. On the other hand, the integral of ω requires the computation of $\Psi(\alpha)$, $\Psi(\beta)$, $\sum \mathrm{Res}(\alpha \int \beta)$, and the tiny integral $\int_Q^{\phi(-Q)} \omega$. As before, the tiny integral is computed with precision as above.

Since $\alpha = \phi^*\omega - p\omega$, we may write $\Psi(\alpha)$ in terms of things we have already computed, namely $\Psi(\alpha) = \mathrm{Frob}(\Psi(\omega)) - p\Psi(\omega)$. So need not do more work here. However, the precision of $\sum \mathrm{Res}(\alpha \int \beta)$ merits further discussion, as we must consider its representation in local coordinates.

6.2.2. *Precision of local coordinates.* Computing with local coordinates is crucial to the algorithm. More precisely, for any point P, we must construct power series $x(t), y(t)$ for a local parameter t such that $P = (x(0), y(0))$. To explicitly compute with power series, we need to know where (t-adically) it is acceptable to truncate them.

6.2.3. *Precision: Cup product matrix.* The first instance this problem arises is in the computation of the cup product matrix. Since $v_t(\omega_j) = 2(g-j) - 2$, which is minimal for $j = 2g-1$, we have $\min v_t(\omega_j) = -2g$. Thus it suffices to compute each basis differential ω_k to a precision of t^{2g}. Consequently, we compute $x(t)$ to a precision of $t^{2(2g-1)}$ and $y(t)$ to a precision of t^{2g-1}.

6.2.4. *Precision: $\sum \mathrm{Res}(\alpha \int \beta)$.* Now we consider $\sum_A \mathrm{Res}_A(\alpha \int \beta)$, where the sum is taken over all points A in the set {poles of α, Weierstrass points of C}. We begin by looking at the expansion for $\alpha = \phi^*\omega - p\omega$.

If A is a non-Weierstrass point defined over $\mathbb{Q}_p$, then computing α in local coordinates is unnecessary, as α just has a simple pole at A. So $\mathrm{Res}_A(\alpha \int \beta) = \mathrm{Res}_A \alpha$, and we may simply read off the residue:

- $A = P$ Teichmüller: $1 - p$
- $A = P$ not Teichmüller: $-p$
- $A = -P$ Teichmüller: $p - 1$
- $A = -P$ not Teichmüller: p.

In the case where A is non-Weierstrass and defined over an extension of $\mathbb{Q}_p$, we have to compute Coleman integrals and local coordinates, so we must study the precision of both, as given by the following corollary of Proposition 6.2:

Corollary 6.4. *Let A be non-Weierstrass, defined over degree p extension k' of $\mathbb{Q}_p$. Let U_A denote the residue disc of A, and let B be a non-Weierstrass point in U_A defined over $\mathbb{Q}_p$. Suppose a working precision of n p-adic digits (so that A has precision pn in a uniformizer π). Let β be written in terms of the local coordinate $(x(t), y(t))$ at B, so that $\beta = h(t)dt$ with $h(t)$ truncated modulo t^{mp}. Then the residue $\sum_{S \in U_A} \mathrm{Res}(\alpha \int \beta)$ has $\min\{n, pm + 1 - \lfloor \log_p(pm+1) \rfloor\}$ digits of precision.*

Proof. If A is non-Weierstrass and defined over an extension K of $\mathbb{Q}_p$, then the contribution of α to the residue calculation just depends on the disc of A: $+1$ if A is in U_P, and -1 if A is in U_{-P}, with the constant of integration fixed in each residue

disc. However, in this case, since we have multiple poles in each residue disc, we must compute $\mathrm{Res}(\alpha(\int_Z \beta)$, where the integral of β is definite, taking into account a constant of integration chosen for each residue disc. More precisely: suppose we are working in the residue disc of P, and say A is defined over a degree p extension of $\mathbb{Q}_p$. Note that we must compute the local coordinates $(x(t), y(t))$ at P with a precision of at least t^{pm}. As the interpolation from P to A is linear, we merely make a linear substitution

$$\begin{aligned} x(t) &:= x((x(A) - x(P))t) \\ y(t) &:= y((x(A) - x(P))t). \end{aligned}$$

This new $x(t), y(t))$ is used to compute the tiny integral of β from P to A, the result of which has precision $\min\{n, pm + 1 - \lfloor \log_p(pm + 1) \rfloor\}$. Taking the trace from K to $\mathbb{Q}_p$ accounts for the other poles of α in the disc of P. □

Finally, in the case where A is a finite Weierstrass point, we have to compute in the local coordinates of A. (Note that we need not compute the residue at $(0, 0)$ if on the curve or at infinity.)

Proposition 6.5. *Let α be above and let A be a finite Weierstrass point not equal to $(0, 0)$. Let $(x(t), y(t))$ represent the local coordinates at A. Then to compute $\mathrm{Res}(\alpha \int \beta)$ with n digits of p-adic precision, we compute $(x(t), y(t))$ to $t^{2pn-p-3}$.*

Proof. We have

$$\begin{aligned} \alpha &= \phi^*\omega - p\omega \\ &= \frac{y(P)px^{p-1}dx}{\phi(y)(x^p - x(P))} - \frac{py(P)dx}{y(x - x(P))}, \end{aligned}$$

where

$$\frac{1}{\phi(y)} = y^{-p} \sum_{i=0}^{\infty} \binom{-1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{f(x)^{pi}}.$$

For $\mathrm{Res}(\alpha \int \beta)$ to have n digits of p-adic precision, we must compute n terms of the binomial expansion of $\frac{1}{\phi(y)}$.

Recall that for a finite Weierstrass point $(a, 0)$, we have

$$\begin{aligned} x(t) &= a + \frac{1}{g(a)}t^2 + O(t^4) \\ y(t) &= t, \end{aligned}$$

where $g(x) = \frac{f(x)}{x-a}$. Note that by hypothesis, $a \neq 0$. We compute the t-adic valuation of α:

$$\begin{aligned} v_t(\alpha) &= v_t(\phi^*\omega) \quad \text{since } \omega \text{ only contributes higher-order terms} \\ &= v_t\left(\frac{y(P)px^{p-1}dx}{\phi(y)(x^p - x(P))}\right) \\ &= 1 + v_t\left(\frac{1}{\phi(y)}\right) \quad (x^p \neq x(P)) \\ &= 1 - pv_t(y) + (n-1)v_t\left(\frac{f(x^p) - f(x)^p}{f(x)^p}\right) \\ &= 1 - p + (n-1)\begin{cases} (2-2p), & \text{if } v_t(f(x^p) - f(x)^p) > 0 \\ -2p, & \text{else} \end{cases} \end{aligned}$$

Thus we have

$$v_t(\alpha) = \begin{cases} p - 2pn + 2n - 1, & \text{if } v_t(f(x^p) - f(x)^p) > 0 \\ p - 2pn + 1, & \text{else.} \end{cases}$$

As $p - 2pn + 2n - 1 \geq p - 2pn + 1$ for $n \geq 1$, we have $v_t(\alpha) \geq p - 2pn + 1$. Set $m = 2pn - p - 1$. Since we want $\mathrm{Res}(\alpha \int \beta)$, we need $v_t(\alpha \int \beta) \geq -1$, so we must compute β to at least t^{m-2}. To get this precision, we must in turn compute with $x(t), y(t)$ to this precision. □

7. Examples

Here we provide some examples of our algorithms.

7.1. **Local heights: genus 2, general divisors.** Let C be the genus 2 hyperelliptic curve

$$y^2 = x^5 - 23x^3 + 18x^2 + 40x = (x-4)(x-2)x(x+1)(x+5)$$

over $\mathbb{Q}_{11}$, and let

$$\begin{aligned} D_1 &= (P) - (Q) \\ D_2 &= (R) - (S), \end{aligned}$$

where $P = (-4, 24), Q = (1, 6), R = (5, 30), S = (-2, 12)$. We describe how to use Algorithm 5.7 to compute the local contribution at $p = 11$.

We see that

$$\begin{aligned} D_1^+ &= \mathrm{div}\left(\frac{x - x(P)}{x - x(Q)}\right), \quad D_1^- = [(P) - (-P)] + [(-Q) - (Q)], \\ D_2^+ &= \mathrm{div}\left(\frac{x - x(R)}{x - x(S)}\right), \quad D_2^- = [(R) - (-R)] + [(-S) - (S)]. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} \frac{1}{4}h_{11}(D_1^+, D_2^+) &= \frac{1}{4}\log\left(\frac{x - x(P)}{x - x(Q)}(D_2^+)\right) \\ &= \frac{1}{2}\log\left(\left(\frac{x(R) - x(P)}{x(R) - x(Q)}\right)\left(\frac{x(S) - x(P)}{x(S) - x(Q)}\right)^{-1}\right) \\ &= 2 \cdot 11 + 9 \cdot 11^2 + 7 \cdot 11^3 + 2 \cdot 11^4 + O(11^5). \end{aligned}$$

Now we compute, using Algorithm 5.8, the contributions from antisymmetric heights (details of which are in Subsection 7.2):

$$h_{11}((P)-(-P),(-S)-(S)) = 9\cdot 11^{-1}+5+6\cdot 11+8\cdot 11^2+9\cdot 11^3+3\cdot 11^4+O(11^5)$$
$$h_{11}((P)-(-P),(R)-(-R)) = 6\cdot 11^{-1}+10+7\cdot 11+6\cdot 11^2+3\cdot 11^3+7\cdot 11^4+O(11^5)$$
$$h_{11}((-Q)-(Q),(R)-(-R)) = 8\cdot 11^{-1}+5+7\cdot 11+10\cdot 11^2+3\cdot 11^3+7\cdot 11^4+O(11^5)$$
$$h_{11}((-Q)-(-Q),(-S)-(S)) = 11^{-1}+8+7\cdot 11+2\cdot 11^2+7\cdot 11^3+8\cdot 11^4+O(11^5),$$

which gives

$$\begin{aligned}\frac{1}{4}h_{11}(D_1^-,D_2^-) = \frac{1}{4}(&h_{11}((P)-(-P),(-S)-(S))+\\ &h_{11}((P)-(-P),(R)-(-R))+\\ &h_{11}((-Q)-(Q),(R)-(-R))+\\ &h_{11}((-Q)-(-Q),(-S)-(S)))\\ &= 6\cdot 11^{-1}+7+4\cdot 11+4\cdot 11^2+3\cdot 11^3+11^4+O(11^5).\end{aligned}$$

Finally, we have

$$\begin{aligned}h_{11}(D_1,D_2) &= \frac{1}{4}h_{11}(D_1^+,D_2^+)+\frac{1}{4}h_{11}(D_1^-,D_2^-)\\ &= 6\cdot 11^{-1}+7+6\cdot 11+2\cdot 11^2+4\cdot 11^4+O(11^5).\end{aligned}$$

7.2. **Local heights: genus 2, antisymmetric divisors.** Keeping notation as in Subsection 7.1, we describe in more detail how to use Algorithm 5.8 to compute the local contribution for one of the antisymmetric divisors:

$$h_{11}((P)-(-P),(R)-(-R)).$$

For ease of notation, let us call these divisors

$$D_P = (P)-(-P), \quad D_R = (R)-(-R).$$

With respect to the standard basis $\mathcal{B}$, the cup product matrix is

$$N = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & -\frac{23}{3} \\ -\frac{1}{3} & 0 & \frac{23}{3} & 0 \end{pmatrix}.$$

Let ν_P be a differential with residue divisor D_P: we have $\nu_P = \frac{24dx}{y(x+4)}$.

We compute $\Psi(\nu_P)$ with respect to the basis $\{\omega_0,\omega_1,\mathrm{Frob}^n\,\omega_2,\mathrm{Frob}^n\,\omega_3\}$:

$$\Psi(\nu_P) = \begin{pmatrix} 8\cdot 11^{-1}+9+6\cdot 11+3\cdot 11^2+7\cdot 11^3+11^4+O(11^5) \\ 7\cdot 11^{-1}+1+4\cdot 11^2+2\cdot 11^3+8\cdot 11^4+O(11^5) \\ 7+9\cdot 11+7\cdot 11^2+4\cdot 11^4+8\cdot 11^5+O(11^6) \\ 2+2\cdot 11+8\cdot 11^2+6\cdot 11^3+7\cdot 11^4+2\cdot 11^5+O(11^6) \end{pmatrix}.$$

This implies that

$$\int_{D_R}\eta_1 = 5\cdot 11^{-1}+6+3\cdot 11+11^3+7\cdot 11^4+O(11^5).$$

To integrate ν_P, we compute several quantities. Noting that $\alpha = \phi^*\nu_P - p\nu_P$ and that the Ψ map is Frobenius equivariant, we have

$$\Psi(\alpha) = \Psi(\phi^*\nu_P - p\nu_P) = \phi^*(\Psi(\nu_P)) - p\Psi(\nu_P).$$

In particular, this makes the computation of $\phi^*(\Psi(\nu_P))$ rather easy, as we have already computed $\Psi(\nu_P)$, and all that is left to do is multiply by the matrix of Frobenius. We find that

$$\Psi(\alpha) = \begin{pmatrix} 6\cdot 11 + 5\cdot 11^2 + 2\cdot 11^4 + 9\cdot 11^5 + O(11^6) \\ 2\cdot 11 + 10\cdot 11^2 + 8\cdot 11^3 + 6\cdot 11^4 + 2\cdot 11^5 + O(11^6) \\ 4\cdot 11 + 6\cdot 11^2 + 2\cdot 11^3 + 11^4 + 9\cdot 11^5 + O(11^6) \\ 3\cdot 11 + 2\cdot 11^2 + 8\cdot 11^3 + 2\cdot 11^4 + 4\cdot 11^5 + O(11^6) \end{pmatrix}.$$

We wish β to have residue divisor D_R, so let $\beta = \frac{30dx}{y(x-5)}$. Then

$$\Psi(\alpha) \cup \Psi(\beta) = 6 + 11^2 + 9\cdot 11^4 + 5\cdot 11^5 + O(11^6).$$

To compute $\sum \mathrm{Res}(\alpha \int \beta)$, we must sum over all Weierstrass point and poles of α. Recall that within a single residue disc, $\sum_A \mathrm{Res}_A(\alpha) = 0$. Now computing the action of Ψ on this differential is slightly more complicated, since instead of just two non-Weierstrass poles, we have $2p = 2\cdot 11$ non-Weierstrass poles: those points in the residue discs of P and $-P$ with x-coordinate $\zeta_{11}^j(-4)^{1/11}$ (where $j = 0, \ldots, 10$). This means we must work over the splitting field $L_{-4} = \mathbb{Q}_{11}(\zeta_{11}, (-4)^{1/11})$ of $x^{11}+4$ over $\mathbb{Q}_{11}$ to compute the local symbols. Since each set of pth roots is Galois conjugate, working over L_{-4} yields

$$\sum_j \langle \nu_1, \omega_i \rangle_{P_j} = \mathrm{tr}_{L_{-4}/\mathbb{Q}_{11}}(\langle \nu_1, \omega_i \rangle_{P_1}),$$

where P_j is the point in the residue disc of P with x-coordinate $\zeta_{11}^j(-4)^{1/11}$. We have the following contribution from the disc of P:

$$10\cdot 11 + 9\cdot 11^2 + 4\cdot 11^3 + 3\cdot 11^4 + 4\cdot 11^5 + O(11^6),$$

and the total contribution from non-Weierstrass points is twice this, or

$$9\cdot 11 + 8\cdot 11^2 + 9\cdot 11^3 + 6\cdot 11^4 + 8\cdot 11^5 + O(11^6).$$

Meanwhile, the sum of contributions from all Weierstrass discs is the following:

$$11 + 4\cdot 11^3 + 6\cdot 11^4 + 11^5 + O(11^6).$$

We compute the tiny integral

$$\int_R^{\phi(R)} \nu_1 = 8\cdot 11 + 11^2 + 8\cdot 11^3 + 2\cdot 11^5 + O(11^6).$$

Putting all of this together, we have

$$h_{11}(D_P, D_R) = 6\cdot 11^{-1} + 10 + 7\cdot 11 + 6\cdot 11^2 + 3\cdot 11^3 + 7\cdot 11^4 + O(11^5).$$

As a consistency check, we also compute $h_{11}(D_R, D_P)$. Here we have

$$\int_{D_P} \nu_R = 2 + 11^3 + 10\cdot 11^4 + 4\cdot 11^5 + O(11^6)$$

and

$$\int_{D_P} \eta_R = 5\cdot 11^{-1} + 2 + 3\cdot 11 + 4\cdot 11^2 + 8\cdot 11^3 + 2\cdot 11^4 + O(11^5),$$

which gives

$$h_{11}(D_R, D_P) = 6\cdot 11^{-1} + 10 + 7\cdot 11 + 6\cdot 11^2 + 3\cdot 11^3 + 7\cdot 11^4 + O(11^5),$$

illustrating symmetry of the local height pairing.

7.3. **Global heights: genus 1.** We give an example of our implementation in genus 1, which allows for comparison of global heights via the algorithm of Mazur-Stein-Tate.

Let C be the elliptic curve

$$y^2 = x^3 - 5x,$$

with $Q = (-1, 2), R = (5, 10)$, so that

$$(Q) - (-Q) = (R) - (-R) = \left(\frac{9}{4}, -\frac{3}{8}\right) =: P.$$

We compute the 13-adic height of P:

- Above 13, the local height $h_{13}((Q) - (-Q), (R) - (-R))$ is
$$2 \cdot 13 + 6 \cdot 13^2 + 13^3 + 5 \cdot 13^4 + O(13^5).$$
- Away from 13, the only nontrivial contribution is at 3, which is $2 \log 3$ (by work of Müller).
- So the global 13-adic height is $12 \cdot 13 + 4 \cdot 13^2 + 10 \cdot 13^3 + 9 \cdot 13^4 + O(13^5)$.

We compare this to Harvey's implementation [Har08] of the Mazur-Stein-Tate algorithm in Sage:

```
sage: C = EllipticCurve([-5,0])
sage: f = C.padic_height(13)
sage: f(C(9/4,-3/8)) + O(13^5)
12*13 + 4*13^2 + 10*13^3 + 9*13^4 + O(13^5)
```

8. Future work

Below we discuss some natural questions arising from our work.

8.1. **Global height pairings.** Ultimately, we would like to compute the global height pairing. To do so, we would again require C to be a curve over a number field K with good reduction at each place v dividing p. We would also need a continuous idèle class character $\chi : \mathbb{A}_K^*/K^* \longrightarrow \mathbb{Q}_p$ and a splitting $H^1(C/K_v) = H^{1,0}(C/K_v) \oplus W_v$ for each place v dividing p. Computing the local heights at those primes v away from p and those above p, the global height would then be the sum of all local heights. When $K = \mathbb{Q}$, the recent Ph.D. thesis of Müller [Mül10] addresses these local heights away from p, and putting together our results, we are able to compute global heights, as shown in Section 7. It would be quite interesting to extend these computations to number fields.

8.2. **Optimizations.** In another direction, it is also of interest to optimize the present algorithm. Currently, the most expensive step is in computing the Laurent series expansion of α in the various Weierstrass local coordinates to reasonably high precision. As we are just interested in the residue of $\alpha \int \beta$, is there a way to make this faster?

8.3. **Comparison with the work of Mazur-Stein-Tate.** When the curve is elliptic, we are able to compare our algorithm for the height pairing with the algorithm of [MST06], as in Section 7. We note that we compute the height pairing for divisors with disjoint support. It is obviously possible to compute without this assumption by replacing one divisor by a linearly equivalent one with this property. But it is also possible to extend the method described in [Gro86, §5]. This extended

method can be compared directly with the method of [MST06], as the height is just the height pairing of a divisor with itself.

References

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic Number Theory (G. Hanrot, F. Morain, and E. Thomé, eds.), Lecture Notes in Computer Science, vol. 6197, Springer, 2010, pp. 16–31.

[Bes00] A. Besser, *Syntomic regulators and p-adic integration. II. K_2 of curves*, Proceedings of the Conference on p-adic Aspects of the Theory of Automorphic Representations (Jerusalem, 1998), vol. 120, 2000, pp. 335–359.

[Bes02] ———, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), no. 1, 19–48.

[Bes04] A. Besser, *The p-adic height pairings of Coleman-Gross and of Nekovář*, Number Theory, CRM Proceedings & Lecture Notes, vol. 36, American Mathematical Society, 2004, pp. 13–25.

[Bes07] A. Besser, *On the computation of p-adic height pairings on Jacobians of hyperelliptic curves*, Sage Days 5, `http://wiki.sagemath.org/days5/sched`, 2007.

[Bes10] ———, *Heidelberg lectures on Coleman integration*, Preprint, 2010.

[CdS88] R. Coleman and E. de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988), no. 2, 239–266.

[CG89] R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, 1989, pp. 73–81.

[Col82] R. F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208.

[Col85] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.

[Col89] ———, *Reciprocity laws on curves*, Compositio Math. **72** (1989), no. 2, 205–235.

[Gro86] B. H. Gross, *Local heights on curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 327–339.

[Gut06] I. Gutnik, *Kedlaya's algorithm and Coleman integration*, M.Sc. Thesis, 2006.

[Har08] D. Harvey, *Efficient computation of p-adic heights*, LMS J. Comput. Math. **11** (2008), 40–59.

[Kau99] I. Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces*, Compositio Math. **115** (1999), no. 1, 37–69.

[Ked01] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338, erratum *ibid.* **18** (2003), 417–418.

[Kob98] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer-Verlag, Berlin, 1998, With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[MST06] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic).

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1.

[Mül10] J. S. Müller, *Canonical heights on Jacobians*, Bayreuth Ph.D. thesis (2010).

[Nek93] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202.

[S$^+$10] W. A. Stein et al., *Sage Mathematics Software (Version 4.5)*, The Sage Development Team, 2010, `http://www.sagemath.org`.

[Sch82] P. Schneider, *p-adic height pairings I*, Invent. Math. **69** (1982), no. 3, 401–409.

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139

Department of Mathematics, Ben-Gurion University of the Negev, P.O.B. 653, Be'er-Sheva 84105, Israel